Science & Society

EMBO reports

E-commerce and biological weapons nonproliferation

Online marketplaces challenge export controls to reduce the risk that rogue states or terrorists could acquire the capacity to produce biological weapons

Raymond A Zilinskas & Philippe Mauger

The 1972 Biological and Toxin Weapons Convention (BWC) was the first international treaty that enjoins nations to outlaw an entire class of weapons of mass destruction. The BWC's Article I bans the development, production, stockpiling, or other acquisition of "microbial or other biological agents, or toxins whatever their origin or method of production, of types and in quantities that have no justification for prophylactic, protective or other peaceful purposes," as well as "weapons, equipment or means of delivery designed to use such agents or toxins for hostile purposes or in armed conflict" (http://www.un.org/disarmament/WMD/Bio/pdf/Text_of_the_Convention.pdf). Given that the treaty has 173 states parties and 9 signatories, most the world's countries are bound by its provisions.

> *"Certain countries, notably the Soviet Union and Iraq, have abused the lack of verification mechanisms in the past to develop biological weapons in breach of their international obligations."*

In practice, however, the BWC lacks provisions for verifying that state parties comply with its strictures. Certain countries, notably the Soviet Union and Iraq, have abused the lack of verification mechanisms in the past to develop biological weapons in breach of their international obligations. Moreover, non-state groups and individuals cannot be expected to follow the treaty's provisions. Therefore, it remains of utmost importance for all states to control the trade of sensitive equipment that can be misused to produce, process, test, and disseminate pathogens and toxins. By doing so, they are in compliance with the BWC's Article III, which forbids states parties to "transfer to any recipient whatsoever, directly or indirectly, and not in any way to assist, encourage, or induce any State, group of States or international organizations to manufacture or otherwise acquire any of the agents, toxins, weapons, equipment or means of delivery specified in Article I". Since the BWC itself has no mechanism by which to enforce Article III, it is up to states parties to put in place effective measures.

Many states have in fact implemented national export controls governing, *inter alia*, the transfer of sensitive biotechnology equipment, pathogens, and toxins. However, to ensure the effectiveness of these controls, 41 states and the European Union (EU) currently harmonize their biological and chemical export control efforts through the so-called Australia Group (AG; http://www.australiagroup.net/en/).

In June 1985, after Iraq used chemical weapons in the Iran–Iraq war (1980–1988), 15 industrialized countries and the EU formed an informal organization with the aim of discouraging and impeding chemical weapons proliferation through the harmonization of national export controls on chemical warfare (CW) materials. Australia proposed the first meeting, hence the group's name. In the early 1990s, the AG's scope was widened to include items that could be used to acquire biological weapons. It developed five export control lists, called the Common Control Lists (http://www.australiagroup.net/en/control-lists.html), that participant states use to guide them when adopting national legislation to control chemical weapons precursors; dual-use chemical manufacturing facilities and equipment and related technology and software; dual-use biological equipment and related technology and software; human and animal pathogens and toxins; and plant pathogens.

> *"E-marketplaces present huge challenges for export control efforts, as they provide visibility and a degree of legitimacy for large and small companies that sell products throughout the world."*

AG participant states are also committed to implement so-called Catch-All measures to cover items that are not explicitly controlled by these lists (http://www.australiagroup.net/en/guidelines.html). "Catch-all" clauses in national legislation inform exporters that if they are aware, or are made aware, that some item "may be intended, in their entirety or part, for use in connection with chemical or biological weapons activities," they must seek an export authorization from the appropriate national authorities.

Middlebury Institute of International Studies, Monterey, CA, USA. E-mail: rzilinskas@miis.edu
DOI 10.15252/embr.201541232 | Published online 12 October 2015

While conducting an earlier study on the threat posed by producers of illicit botulinum toxin products, we found that a profusion of such products was readily available from vendors over the Internet [1]. This caused us to wonder whether sensitive biotechnology equipments that meet the requirements for export control were similarly easily available from Internet vendors. To test whether this was so, we conducted a scoping study to document the availability of AG-controlled equipment online and published the results in an occasional paper [2]. The findings were that the growth in biotechnology e-commerce had created serious export control issues. The current article accordingly seeks to generate interest and awareness among scientists and arms control experts of the fact that e-commerce makes it much easier for anyone interested—be it state actors, groups, or individuals—to acquire equipment that could be used to produce biological weapons whose payloads were pathogens or toxins.

"Strategic trade control specialists have already raised concerns that legal online procurement networks can be abused by proliferators to acquire sensitive equipment…"

This article is limited to equipment listed by the AG for control on the dual-use biological equipment and related technology and software Common Control List (henceforth "Biological Equipment List"; http://www.australiagroup.net/en/dual_biological.html). The list has nine categories of equipments, along with related technology and software: complete containment facilities at the BSL-3 and BSL-4 levels; fermenters; centrifugal separators; cross (tangential) flow filtration equipment; freeze-drying equipment; spray-drying equipment; protective and containment equipment; aerosol inhalation chambers; and spraying or fogging systems and components thereof.

Each of these items is dual-use; that is, it can be used for both civilian and military applications. That being the case, only items that possess certain particularly sensitive characteristics are subject to export controls. For example, not all fermenters are regulated under the Biological Equipment List, but only those that are "suitable for the cultivation of pathogenic microorganisms or of live cells for the production of pathogenic viruses or toxins without the propagation of aerosols" and that have a capacity of 20 liters or more. Hereafter, we refer to items that the AG singles out for export control as "AG-grade items". Of the nine categories listed above, we selected categories 2–9 as subjects for our research, as item 1 on the list—high-end containment facilities—is unlikely to be of interest to terrorists.

Online sales of production equipment usually take place through two types of business-to-business (B2B) websites: e-catalogs and e-marketplaces. E-catalogs replace printed catalogs from manufacturers or companies that trade in used and surplus equipment. An e-catalog simply lists tradable items with information and prices on a website. A sale through such a website typically has two parties: the website owner who sells the product, and the buyer. The use of e-catalogs to effect sales does not depart significantly from typical export–import trading between companies.

In contrast to e-catalogs, e-marketplaces, such as eBay and Alibaba, are facilitation platforms where numerous companies advertise their products or services and where prospective buyers enquire after specific products or services. A single sale through an e-marketplace B2B website typically involves three parties: the website owner acting as a facilitator, the vendor, and the buyer. An active e-marketplace will have many different vendor–buyer pairs carrying out transactions simultaneously.

E-marketplaces present huge challenges for export control efforts, as they provide visibility and a degree of legitimacy for large and small companies that sell products throughout the world. In the past, companies would have to dispatch trade delegations or join trade fairs to demonstrate the merits of their products to prospective customers. The existence of e-marketplaces has reduced the necessity of doing so. More broadly, e-marketplaces have reduced the need for marketing, dependence on brand recognition, and the costs of selling internationally. E-marketplaces have created an international supplier base of small, low-volume companies that did not exist in the pre-Internet era.

A growing online trade in a wide range of illegal products, such as unlicensed firearms, botulinum toxin products, and illegal drugs [1,3–5] is now taking place through dedicated—and hence illegal—e-marketplaces. Online purchases of AG-sensitive equipment pose an even more difficult challenge for law enforcement agencies because, unlike weapons, drugs, or counterfeit products, such equipment is rarely illegal *per se*. All items on the Biological Equipment List have legitimate uses, and e-marketplaces used to trade such products are therefore entirely "aboveground".

"Nowadays, e-commerce would greatly facilitate a modern version of Iraq's covert networks for purchasing dual-use products of concern."

Strategic trade control specialists have already raised concerns that legal online procurement networks can be abused by proliferators to acquire sensitive equipment and supplies for missile, chemical weapons, and nuclear weapons programs. In 2014, a US National Academy of Sciences committee warned of CW-related equipment being sold through B2B websites [6]. In the UK, King's College London's Project Alpha demonstrated how B2B websites could be exploited for missile and nuclear technology proliferation. One Project Alpha study documented that, at the time they were conducting their research, a sanctioned missile-related entity had a listed seller profile on no less than 15 Internet trading platforms, and 5 sanctioned Iranian companies were advertising on Alibaba, probably the world's largest B2B website (https://www.acsss.info/proliferation/item/370-the-great-takedown-alibaba-com-delists-factory-owned-by-notorious-missile-proliferator). Project Alpha also highlighted vendors that offered specific metals and subcomponents suitable for the manufacture of centrifuges and centrifuge cascades for uranium enrichment, specialized machining, and photographic equipment suitable for use in a nuclear weapons program, and even "an ad for the sale of the rare metal gallium, which the vendor trumpeted could be used to stabilize plutonium" [7]. The project staff demonstrated the seriousness of the problem by successfully purchasing a controlled MKS

pressure transducer from a Chinese firm through eBay, and publicized the fact that the Chinese firm had not sought end user information and hence probably had failed to seek an export license (https://www.acsss.info/proliferation/item/321-procurement-of-pressure-transducer-via-ebay-from-china). As Project Alpha's staff concluded, these findings demonstrated "the need to rethink how Internet trading platforms ensure that they are not used as platforms that enable proliferation" (https://www.acsss.info/proliferation/item/321-procurement-of-pressure-transducer-via-ebay-from-china).

Given these results, and in view of our preliminary research, we hypothesized that the ready availability of biotechnology equipment offered through B2B websites allowed potential proliferators to purchase every item listed on the Biological Equipment List. We sought to test this hypothesis by contacting companies selling dual-use equipment of concern. We searched through more than 30 e-marketplaces and identified 61 companies that offered what appeared to be AG-grade items in six of the eight AG Biological Equipment List categories.

Table 1. AG item search results.

Equipment type		Availability through internet vendors
AG Item 2	Fermenters	Plentiful
AG Item 3	Centrifugal separators	Rare
AG Item 4	Cross or tangential flow filtration systems	Rare
AG Item 5	Freeze dryers	Plentiful
AG Item 6	Spray dryers	Common
AG Item 7	Protective and containment equipment	Class III biosafety cabinets plentiful
AG Item 8	Aerosol inhalation chambers	Rare, domestically oriented sales
AG Item 9	Spraying or fogging systems and components	None found that fulfill AG requirements

The number of vendors found in each category varied widely. In Table 1, we list types of equipment and their availability using general terms. Thus, by "plentiful," we mean that the equipment was offered by many vendors. By "rare," we mean that only a handful vendors for that particular item were found and that it was difficult to determine whether these items were AG-grade or not. We used "common" to describe the availability of spray dryers, because we found many vendors, but it was not easy to determine whether the items they were selling were AG-grade.

We found that many companies not only sold AG-grade equipment but also proffered some degree of assistance, ranging from on-site installation to training personnel on their use. Buyers could therefore count on technical guidance by the vendor's experts in person, or through B2B chat services, direct emails, and telephone conversations. Thus, for example, a would-be proliferator content with acquiring a low-level BW capability might obtain what was required by paying for the on-site installation and calibration of a small turnkey fermenter and centrifuge setup, as well as for the training of their personnel in the setup's operation as per its supposed civilian cover. Although subsequent adjustments would have to be made to convert the line to non-civilian use, a proliferator that picked the right equipment and asked for the right type of cover story training could be in a position to propagate and process pathogenic and toxigenic bacteria.

"Unlike large and well-established companies, Internet vendors who now sell products of concern might not ask so many questions."

We were not able to conduct "sting" purchases—such as Project Alpha was able to do with the MKS pressure transducer—to test whether we could obtain sensitive items without providing appropriate end user information. To compensate for this shortcoming, we specifically searched for sellers in non-AG countries where export controls can be expected to be weaker than in AG-member counterparts. We found 61 vendors of probable AG-grade equipment. Of these, 60 were outside of the USA and EU and 57 were in non-AG countries. We noted that several of the 61 companies were small; 20 had 50 or fewer employees and some had fewer than 10. Small companies typically lack the resources to conduct extensive know-your-customer checks as part of a diligent export control process. We also analyzed payment methods and found that many companies advertised at least one method (usually Western Union) that allows buyers to remain anonymous [8], although other methods that allow varying degrees of concealment could also be used (Fig 1).

We contacted some of the documented companies, but were not able to obtain information about their export procedures. The e-marketplace site Alibaba did list the relevant regulations regarding dual-use biotechnology exports, but given the sheer number of active vendors, a would-be proliferator could probably still find a seller that is unaware of, or willing to ignore, these regulations. We actually observed a would-be buyer posting a notice on Alibaba that they wished to purchase a 50- to 60-liter fermenter for personal use. In reply, a number of companies indicated that they were willing to sell whatever the buyer required, offering even larger fermenters of up to 30,000 liters. None of the willing vendors appeared to be interested in learning about the buyer, nor for what purpose would the fermenter be used. Further, none of the 61 vendors noted above mentioned anything about regulations or any other possible impediments to the transaction. We found only one vendor—which was not among the 61 documented vendors and was based in the USA—explicitly noted that its goods would only be "sold to pharmaceutical or chemical manufacturers" and only after proper authorization.

To illustrate how biotechnology e-commerce challenges export control measures, we briefly discuss Iraq's procurement network for BW-related items as it existed in the late 1970s through the early 1980s, which has been described in detail by the United Nations Monitoring, Verification, and Inspection Commission (UNMOVIC) [9]. We then portray how a contemporary proliferator could harness the Internet to establish an efficient procurement network.

When Iraq began acquiring BW-relevant equipment in the mid-1970s, there were few export controls in place to prevent it from acquiring biological and chemical equipment and supplies. The Iraqi procurement network at that time was simple: The solicitor

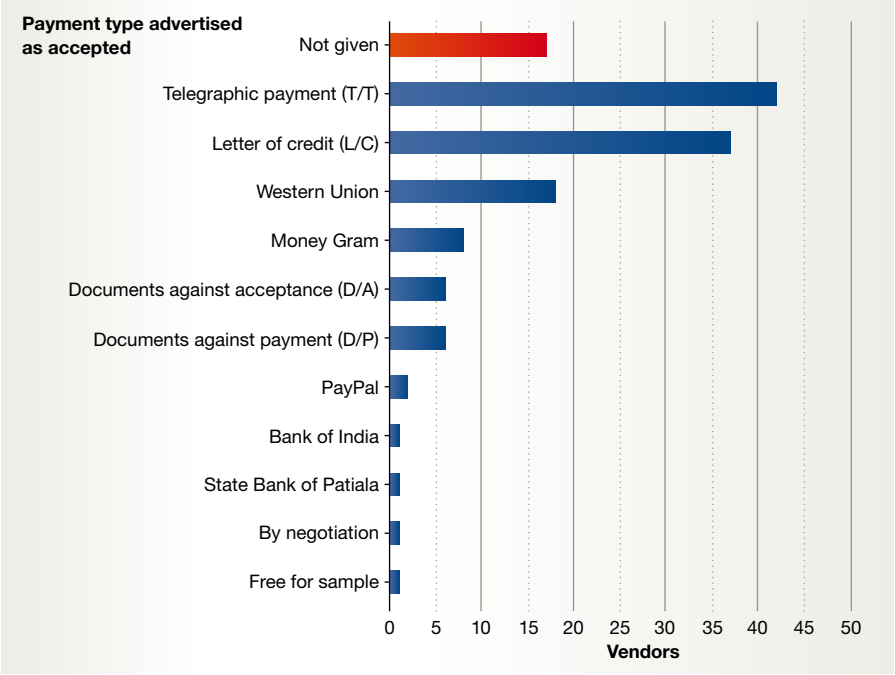

Figure 1. Number of vendors advertising a particular payment option.

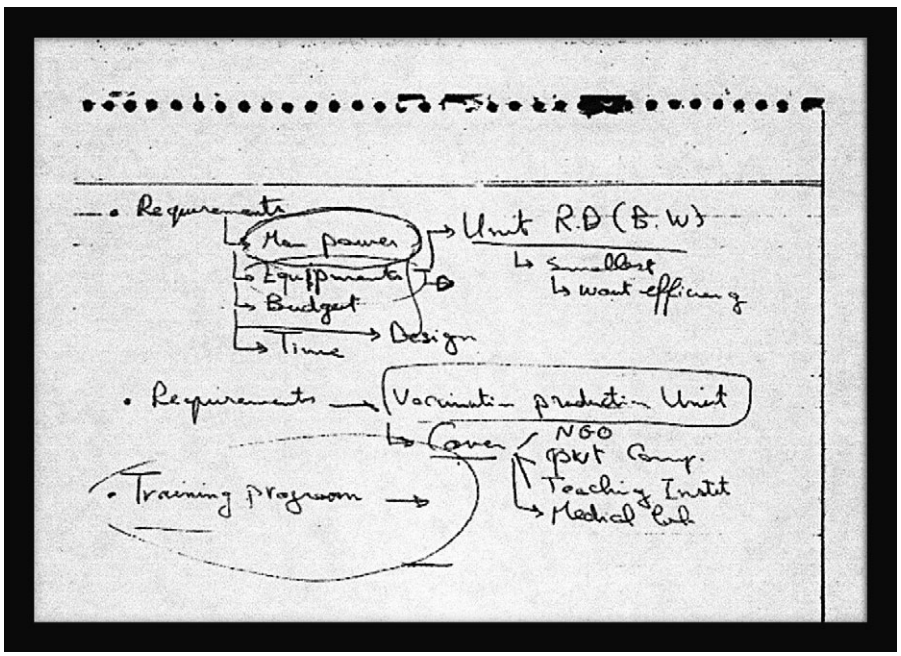

Figure 2. Elements for an Al Qaeda biological weapons facility.
Abdur Rauf Ahmed spells out the five basic requirements needed to set up a BW research and development unit: manpower, equipment, budget, design (presumably for the facility), and time (presumably for construction benchmarks). The BW facility's cover would be that it is a "vaccination production unit" that is supposedly operated by an NGO, government company, teaching institute, or medical laboratory.

and the potential supplier were in direct contact throughout the entire deal, the money was transferred from Iraq to foreign banks, and the supplier shipped the purchased item to Iraq. In the mid-1980s, the industrialized nations recognized that Iraq had been able to establish a significant chemical weapons program after having purchased the equipment, chemical precursors, and protective gear mostly from Western companies. By the late 1980s, new AG-coordinated export controls were in place, and Iraq's chemical and biological weapons acquisition programs were significantly disrupted. For example, in 1988, its attempts to purchase large-size fermenters and spray dryers for the Al Hakam biological production facility failed. Iraq then established complex, covert acquisition networks to bypass these export controls. Legitimate Iraqi commercial organizations, as well as government ministries and trading agencies, were used as fronts; middlemen in third countries were employed to hide the identity of the end country from vendors; transshipments were orchestrated to further obscure an item's real destination; and ostensibly civilian Iraqi governmental agencies and their officials abroad were used to move and disburse money. These methods worked to some extent, but Iraq's procurement process became much slower and more expensive than in earlier times.

Nowadays, e-commerce would greatly facilitate a modern version of Iraq's covert networks for purchasing dual-use products of concern. A bare-bones model of covert illicit acquisition might look like this: the proliferator sets up a front that has the appearance of a legitimate business and that acts as a customer; the proliferator's solicitor searches for suppliers of new or used equipment, whether in an AG or in a non-AG country; the item is purchased via an Internet connection; and the item is paid for in a hard-to-track fashion. The front company can be situated in a busy transshipment port in a non-AG country, for instance, in Hong Kong, China, to enable reshipment to a sanctioned country. In order to demonstrate how Internet trading has made each of these steps easier, we discuss in more detail how a proliferator could obtain an AG-grade freeze dryer for production of, *inter alia*, a dry *B. anthracis* formulation.

A would-be proliferator could search for suitable freeze dryers on the Internet, note which commercial applications are advertised, and then establish a front company that claims to produce dried fruits and vegetables, instant coffee, or any other of the myriad dried or frozen products found

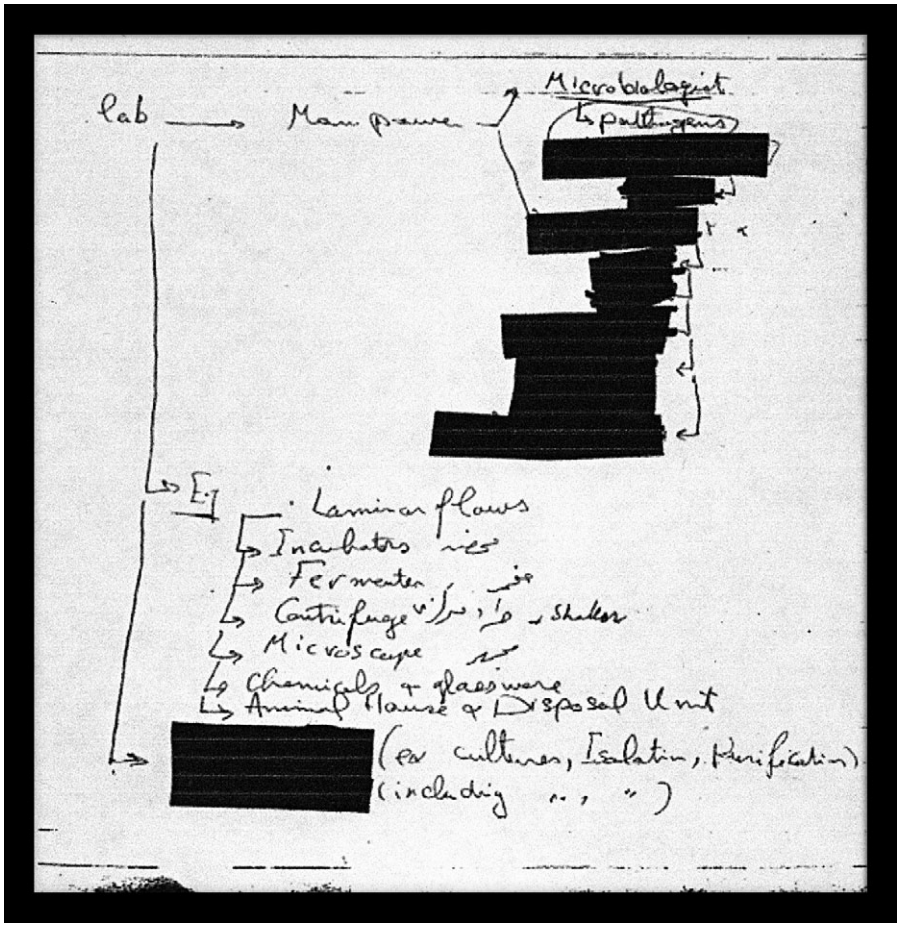

Figure 3. Requirements for work force, equipment, and facilities for an Al Qaeda biological weapons facility.

The work force list is heavily redacted; the only readable entry is for a microbiologist who deals with pathogens. The equipment list includes several items that could be AG-rated, such as the fermenter, the laminar flow safety cabinet, and the centrifuge (albeit not batch-type centrifuges). As for facilities, Abdur Rauf Ahmed provides three examples of presumed laboratories for culturing, isolation, and purification.

in markets throughout the world, which would justify acquiring a particular freeze dryer model. Next, they could go to B2B e-marketplaces and search for suppliers of this model or post their interest in acquiring one on the marketplace and wait for offers. The would-be proliferator could connect with the vendors who ask few questions, offer the best deal, and accept a payment method that shields the buyer's identity. Many companies already list payment methods on their website, which means that the proliferator would not have to inquire into alternate payment methods, which would risk raising a "red flag." To return to our example, we found large, high-quality AG-grade freeze-drying units being offered for < US$115,000 (excluding shipping) from vendors that accept hard-to-trace methods of payment.

The last stage of a transaction, and the last chance for export control measures to have an effect, involves the shipment of the purchased item to the buyer. Shipping costs are typically covered by the buyer, while the vendor organizes the shipment. A diligent would-be proliferator would look for a vendor unconcerned by export license requirements, who would simply ship the item to its destination without further ado. If the would-be proliferator were able to procure the item from a vendor in a non-AG-participating country, the vendor might not even be aware of the item's dual-use nature. Moreover, even diligent vendors can be fooled by a proliferator. Because of the rapid growth of the biotechnology industry, small start-up companies and low-volume traders and resellers of equipment have become very common, which makes it very difficult to distinguish a legitimate business from an illicit procurement network.

To complete this scenario, a would-be proliferator can also acquire parts for AG-grade items from Internet vendors. Access to spare parts is an important element for establishing a proliferation network for three reasons. First, it helps the proliferator to maintain equipment in working condition. For instance, if the freeze dryer's controller broke down, they could easily source a spare through a vendor listed on Alibaba. This may not be of concern for a terrorist group attempting to produce a sufficient quantity of pathogens to mount a one-time attack, but would be important for developing a production line for BW agents. Second, it enables proliferators to buy used, obsolete, or damaged units second-hand and keep them in working condition. Third, a clever technician or engineer could bypass export controls by purchasing individual item sub-components from multiple vendors, and then assemble their own controlled item over time. Given their ubiquity, parts can hardly be controlled by national authorities, perhaps except for a few critical subcomponents identified on the AG list.

Currently, the AG participant states devote significant resources to maintaining export controls on equipment to prevent the production and use of biological weapons. The advent of the Internet, in particular e-commerce, has had a major disruptive effect on these controls, with implications for interdicting biological weapons. Unlike large and well-established companies, Internet vendors who now sell products of concern might not ask so many questions. Nearly all of the vendors we documented in our study were deliberately selected for their location in non-AG participant states: primarily China, India, and Russia. We noted that the sellers were often small and probably lacked the resources to conduct extensive customer checks as part of a diligent export control process. Moreover, we did not discern whether management of these companies actually knew they were selling dual-use items.

To underscore the importance of biotechnology export controls, we conclude this article by relating the sobering story of Pakistani microbiologist Abdur Rauf Ahmed, who worked for Al Qaeda in Afghanistan. In 2001, US forces captured some of his

correspondence and notebooks, which roughly detail how to set up a rudimentary BW facility (Figs 2 and 3). His plans included various cover story options. Of direct relevance to this article are the contents of one of his partly redacted letters: "...successed [sic] in obtaining some of the important internet connections and tried to solve technical problems of our work [...] the complete unit of fermenter along with accessories was in its final stages of its completion [...] I finalised all the accessories required for the smooth running of our bioreacter [sic]...I am sending you a final price list of items to be shipped" (https://caseclosedbylewweinstein.wordpress.com/2012/08/26/excerpt-on-rauf-ahmed-abdur-rauf-from-2012-georgetown-phd-thesis/).

We do not know from where Abdur Rauf Ahmed sourced the bioreactor and its accessories, nor the specifics of "internet connections." However, we can consider a reasonable scenario: The equipment could have been ordered online using a fake laboratory as cover, located in a neighboring country such as Pakistan or Tajikistan. The equipment could then have been transported by an overland vehicle to Rauf Ahmed's real location in Afghanistan. If this is what happened, it would have been very difficult for an outsider to find out where the items ended up and who the end user was. We fear that if nothing is done to adapt current BW-related interdiction efforts to the Internet age, we may well see the next proliferator being able to realize this scenario.

Acknowledgements

The project whose findings are reported in this article was funded by the British Foreign and Commonwealth Office. This article is an abridged and modified version of [2].

Conflict of interest

The authors declare that they have no conflict of interest.

References

1. Coleman K, Zilinskas RA (2010) Fake Botox, real threat. *Sci Am* 302: 84–89 (June 2010). http://www.scientificamerican.com/article.cfm?id=fake-botox-real-threat
2. Zilinskas RA, Mauger P (2015) *Biotechnology E-commerce: a Disruptive Challenge to Biological Arms Control*. Monterey, CA: James Martin Center for Nonproliferation Studies, Occasional Paper No. 21. http://www.nonproliferation.org/biotechnology-e-commerce-a-disruptive-challenge-to-biological-arms-control/
3. Levin D (2015) In China, illegal drugs are sold online in an unbridled market. *New York Times*, June 21. http://www.nytimes.com/2015/06/22/world/asia/in-china-illegal-drugs-are-sold-online-in-an-unbridled-market.html?_r=0
4. Randewich N (2013) New Silk Road drug bazaar opens a month after FBI bust. *Reuters*, November 7. http://www.reuters.com/article/2013/11/07/us-crime-silkroad-idUSBRE9A608I20131107
5. Seelow S (2013) Un vaste réseau international de trafic d'armes démantelé en France" (a vast international arms trafficking network dismantled in France), *Le Monde*, December 2. http://www.lemonde.fr/societe/article/2013/12/02/un-vaste-reseau-international-de-trafic-d-armes-demantele-en-france_3524283_3224.html.
6. Hughes K, Alper J (2014) *The Global Movement and Tracking of Chemical Manufacturing Equipment: a Workshop Summary*. Washington, DC: National Academies Press, pp 23–25. http://www.nap.edu/catalog/18820/the-global-movement-and-tracking-of-chemical-manufacturing-equipment-a
7. Stewart IJ, Gillard N, Brewer J (2014) Internet-trading platforms: Making it easier to get around sanctions? *Bulletin of the Atomic Scientists*, October 31. http://thebulletin.org/Internet-trading-platforms-making-it-easier-get-around-sanctions7772
8. Madinger J (2012) *Money Laundering: a Guide for Criminal Investigators*. Boca Raton: CRC Press
9. United Nations Monitoring, Verification and Inspection Commission (UNMOVIC) (2005) Chapter V: the biological weapons programme. *Compendium of Iraq's Proscribed Weapons Programmes in the Chemical, Biological and Missile Areas*. New York, NY: United Nations

